Moaaz Abouobaida

L2 SOC Analyst | Security & Systems Engineer

Al Rawdah, Riyadh 13213, Saudi Arabia • +966 53 583 9579 • moazabuobida17ca@gmail.com
linkedin.com/in/moaaz-abouobaida • moazabuobida.xyz

PROFESSIONAL SUMMARY

Cybersecurity professional and L2 SOC Analyst with 8+ years across system administration, network security and infrastructure, and proven experience architecting, deploying and managing Security Operations Centers from the ground up. Founded and currently leads a full cybersecurity department in Saudi Arabia, spanning SOC/SIEM operations, vulnerability management, secure access and security policy, and operates the organization's ISO/IEC 27001:2022-certified Information Security Management System. Adept with advanced SIEM platforms, secure network architecture and complex threat analysis, combining a strong business-risk and auditing foundation with deep technical expertise in endpoint security and traffic analysis.

CORE COMPETENCIES

Security Operations: SOC build-out & management, L2 incident analysis, SIEM deployment (Wazuh), threat hunting, EDR, log analysis & forensics

Network & Infrastructure: MikroTik firewall design, advanced routing, high-availability dual-WAN failover, traffic shaping, VLANs, Windows Server & Active Directory, Microsoft 365

Secure Communications: Enterprise VPN (WireGuard, OpenVPN), secure VoIP (Asterisk / Issabel / FreeSWITCH), SIP dial-plan hardening

Risk, Governance & Compliance: ISO/IEC 27001:2022 ISMS operation & surveillance-audit readiness, IT security auditing, risk register development, vulnerability assessment (Nessus), business impact analysis, NIST CSF, user access & privileged access reviews, security policy authoring

Cloud & Analysis: Azure & AWS security, Microsoft Sentinel & KQL, Wireshark

Programming & Automation: Python, PowerShell, Bash, SQL, C#, JavaScript

PROFESSIONAL EXPERIENCE

Founder & Head of Cybersecurity Department
Nov 2025 – Present

Nataaj AlMutaqaddimah for Information Technology | ERTAQY Software for Business Development — Riyadh, Saudi Arabia

- Established the company's cybersecurity department from the ground up on 1 November 2025, defining its structure, scope of service, tooling stack and operating procedures.
- Built the SOC/SIEM capability on Wazuh, covering log-source onboarding, custom detection rule development and alert triage and escalation workflows.
- Authored the security policies, procedures and technical baselines now applied across internal infrastructure and managed client environments.
- Manage and maintain the ISO/IEC 27001:2022-certified Information Security Management System, sustaining control ownership, documentation and evidence, and readiness for annual surveillance audits.
- Introduced vulnerability management and periodic security review cycles, tracking identified risks through to verified remediation.
- Lead and mentor junior engineers on security operations, escalation paths and incident handling.

The department was established as an internal security function serving the company's own infrastructure and existing client base. It is not operated as a separate commercial entity and does not compete for external tenders.

System Administrator & Technical Support Leader
Nov 2022 – Nov 2025

ERTAQY Software for Business Development — Riyadh, Saudi Arabia

- Maintained core IT infrastructure including servers, network devices and security controls.
- Led a technical support team resolving 500+ incidents annually.
- Administered Windows Server, managed user access, and applied security updates and patch management.
- Implemented firewall rules, VPN configurations and network segmentation to strengthen the security posture.
- Improved system resilience through enforced backup strategies and security policies.

SOC Lead & Infrastructure Security Engineer
2022 – Present

Independent / Project-Based

- Designed and deployed a functional Security Operations Center end-to-end for client networks, from architecture through to live monitoring.
- Engineered and deployed Wazuh SIEM across enterprise networks, authoring custom detection rules and analyzing telemetry from multiple endpoints.
- Architected resilient MikroTik environments with complex port forwarding, traffic shaping and dual-WAN automated failover to guarantee near-zero downtime.
- Packaged and delivered security service tiers spanning threat monitoring, secure remote access and perimeter defense.

Freelance Cybersecurity & Systems Engineer 2022 – Present

Upwork

- Provide international consulting across three pillars: SOC/SIEM implementations (Wazuh), secure remote access (VPNs) and enterprise VoIP (Asterisk / FreeSWITCH).
- Perform deep-dive troubleshooting on SIP dial plans, network bottlenecks and secure data-transmission protocols.
- Design custom security architectures that bridge business-continuity requirements with strict technical controls.

IT Support Specialist & Software Tester Oct 2019 – Nov 2022

Al-Abdellatif Altarshouby Pharmacies

- Delivered IT support and security for 30+ branches, hardening POS and network devices.
- Deployed endpoint protection and password policies across multiple sites.
- Performed QA testing and security checks on new ERP software modules.
- Ensured secure connectivity for remote branches via VPN.

IT Support Technician (Military Service) Jan 2018 – Mar 2019

Egyptian Naval Forces — Financial Department

- Delivered hardware and software support for critical financial systems.
- Ensured secure daily operations through proactive maintenance and troubleshooting.

KEY PROJECTS & HANDS-ON LABS

- **Risk Register & NIST CSF Assessment —** Built a risk register for a financial institution, scoring major threats including business email compromise, database compromise and supply-chain disruption, and produced a prioritization matrix aligned with NIST CSF.
- **Vulnerability Assessment Lab (2023 – Present) —** Built a virtualized enterprise environment in VirtualBox; ran credentialed Nessus scans against intentionally vulnerable systems, performed full audits and implemented remediation that measurably strengthened security posture.
- **WireGuard VPN Infrastructure (VPS) —** Deployed a full WireGuard infrastructure on an international VPS with key management, /32 peer segmentation, firewall whitelisting, DNS overrides and end-to-end testing for secure, high-performance geo-distributed access.
- **OpenVPN on MikroTik —** Built a production-grade OpenVPN server using a static public IP, certificate-based authentication, NAT/firewall policies and optimized routing for secure home-lab remote access.
- **Network Fundamentals Course (2025 – ongoing) —** Designed and delivered a self-paced, security-first networking course for IT beginners.

EDUCATION

M.Sc. Computer Science 2024 – 2028 (in progress)

Cairo University, Egypt

B.Sc. Accounting (Bachelor of Commerce) 2014 – 2017

Mansoura University, Egypt

Financial and auditing foundation that strengthens IT risk assessment, compliance, and translating technical cyber threats into quantifiable business impact.

CERTIFICATIONS

Completed

- CompTIA Security+ (SY0-701)
- Google Cybersecurity Professional Certificate
- CCNA — Cisco Certified Network Associate
- MCSA — Microsoft Certified Solutions Associate

Training Completed / Exam Scheduled

- Microsoft SC-200 — Security Operations Analyst (exam scheduled)
- Microsoft SC-500 — Secure Cloud & AI Solutions (exam scheduled)
- ISO/IEC 27001 Lead Implementer — full course completed, exam pending

Roadmap

eJPTv2 (INE) · AWS Certified Security – Specialty · Google Professional Cloud Security Engineer · CISA (ISACA)

LANGUAGES

Arabic (Native) · English (Fluent — IELTS 7.0) · German (Beginner) · French (Beginner) · Nationality: Egyptian